

CLAIMS

What is claimed is:

SwD
B1

1. An article of manufacture including a sequence of instructions stored
on a computer-readable media which when executed by a network node cause
the network node to perform the acts of:

4 modifying an alert variable based on data transmissions originating from
5 one or more suspect nodes;

6 triggering a first response when said alert variable reaches a first
7 predetermined threshold level; and

8 triggering a second response when said alert variable reaches a second
9 predetermined threshold level.

1 2. The article of manufacture as claimed in claim 1 further including the
2 step of triggering additional responses when said alert variable reaches one or
3 more additional threshold levels.

1 3. The article of manufacture as claimed in claim 1 wherein one of said
2 triggered responses includes a passive scan of one or more of said suspect nodes.

1 4. The article of manufacture as claimed in claim 3 wherein said passive
2 scan includes the step of recording data transmissions in a log file.

1 5. The article of manufacture as claimed in claim 1 wherein one of said
2 triggered responses includes an active scan of one or more of said suspect nodes.

1 6. The article of manufacture as claimed in claim 5 wherein said active
2 scan includes the step of retrieving information about one or more of said
3 suspect nodes including the network address of said suspect nodes.

1 7. The article of manufacture as claimed in claim 5 wherein said active
2 scan includes the step of determining the network route taken by data
3 originating from one or more of said suspect nodes.

1 8. The article of manufacture as claimed in claim 1 wherein one of said
2 triggered responses includes said network node requiring increased
3 authentication from any other node before providing access to its resources.

1 9. The article of manufacture as claimed in claim 8 wherein said
2 increased authentication includes the step of forcing two or more logins before
3 providing access to its resources.

1 10. The article of manufacture as claimed in claim 1 wherein one of said
2 triggered responses includes the step of blocking incoming data transmissions.

1 11. The article of manufacture as claimed in claim 1 wherein said alert
2 variable responds differently over time to particular types of data transmissions.

1 12. The article of manufacture as claimed in claim 11 wherein said alert
2 variable continuously increases in response to the continuous receipt of a
3 particular type of data transmission until the alert variable reaches a
4 predetermined value.

1 13. The article of manufacture as claimed in claim 12 wherein said
2 particular type of data transmission originating from said suspect node is an
3 invalid login attempt.

1 14. The article of manufacture as claimed in claim 11 wherein said alert
2 variable initially increases in response to the continuous receipt of a particular
3 type of data transmission and subsequently decreases in response to the
4 continued receipt of said particular type of data transmission.

1 15. The article of manufacture as claimed in claim 14 wherein said
2 particular type of data transmission originating from said suspect node is a
3 transmission which retrieves information about said network node (e.g., the
4 "ping" command).

1 16. The article of manufacture as claimed in claim 1 wherein said data
2 transmissions are analyzed by said network node on a network packet level.

1 17. The article of manufacture as claimed in claim 16 wherein said data
2 transmissions are filtered by said network node on a network packet level.

1 18. An article of manufacture including a sequence of instructions stored
2 on a computer-readable media which when executed by a network node cause
3 the network node to perform the acts of:

4 modifying a first suspect-specific alert variable based on data
5 transmissions originating from a first suspect node; and

6 modifying a second suspect-specific alert variable based on data
7 transmissions originating from a second suspect node; and

8 triggering a suspect-specific response when either of said suspect-specific
9 alert variables reach a predetermined threshold level.

1 19. The article of manufacture as claimed in claim 18 including the act of
2 triggering additional suspect-specific responses when either of said suspect-
3 specific alert variables reaches additional predetermined threshold values.

1 20. The article of manufacture as claimed in claim 18 including the act of
2 modifying an overall alert variable based on said data transmissions originating
3 from each of said suspect nodes.

1 21. The article of manufacture as claimed in claim 20 including the act of
2 triggering a response towards each one of said plurality of suspect nodes when
3 said overall alert variable reaches a predetermined threshold value.

1 22. The article of manufacture as claimed in claim 20 wherein said overall
2 alert variable is more responsive to new types of data transmissions than to data
3 transmissions previously received at said network node.

1 23. The article of manufacture as claimed in claim 22 including the act of
2 initially increasing said overall alert variable in response to data transmissions
3 originating from a particular suspect node and subsequently decreasing said
4 overall alert variable upon continued receipt of said data transmissions from said
5 particular suspect node.

1 24. The article of manufacture as claimed in claim 18 including the act of
2 communicating each of said suspect-specific alert variables to a network
3 database residing on a server node.

1 25. The article of manufacture as claimed in claim 20 including the act of
2 communicating said overall alert variable to a network database residing on a
3 server node.

1 26. An article of manufacture including a sequence of instructions stored
2 on a computer-readable media which when executed by a network server node
3 cause the network server node to perform the acts of:

4 storing a plurality of suspect-specific alert variables for a plurality of
5 network nodes;

6 modifying a network alert variable based on the value of each of said
7 plurality of suspect-specific alert variables; and

8 triggering a network response when said network alert variable reaches a
9 predetermined threshold level.

1 27. The article of manufacture as claimed in claim 26 wherein said
2 network response includes the act of notifying each of the plurality of network
3 nodes that they should each increase their suspect-specific alert variable towards
4 a particular suspect node.

1 28. The article of manufacture as claimed in claim 27 wherein said
2 network response includes the act of said network server node initiating a
3 passive scan of a particular suspect node.

1 29. The article of manufacture as claimed in claim 27 wherein said
2 network response includes the act of said network server node initiating an
3 active scan of a particular suspect node.

1 30. The article of manufacture as claimed in claim 29 wherein said
2 network response includes the act of blocking all communication between said
3 suspect node and said plurality of network nodes.

1 31. An article of manufacture including a sequence of instructions stored
2 on a computer-readable media which when executed by a network server node
3 cause the network server node to perform the acts of:

4 storing a plurality of overall alert variables for a plurality of network
5 nodes;

6 modifying a network alert variable based on the value of each of said
7 plurality of overall alert variables; and

8 triggering a network response when said network alert variable reaches a
9 predetermined threshold level.

1 32. A method comprising:

2 receiving a first event from a suspect node;

3 recording said first event in a first data structure having an event count
4 value;

5 receiving a second event from said suspect node, said second event being
6 of a same type as said first event; and

7 recording said second event in said first data structure and incrementing
8 said count value if said second event occurs within a predetermined window of
9 time after said first event.

1 33. The method as claimed in claim 32 further comprising recording said
2 second event in a second data structure having a count value if said second event
3 occurs outside of said predetermined window of time after said first event.

1 34. The method as claimed in claim 33 wherein said predetermined
2 window of time is increased responsive to said second event occurring outside of
3 said predetermined window of time.

1 35. The method as claimed in claim 32 wherein said predetermined
2 window of time is modified based on said first or second event type.

1 36. The method as claimed in claim 35 wherein said window of time is
2 increased for more serious event types and decreased for less serious event
3 types.

1 37. The method as claimed in claim 36 wherein said event type is an
2 invalid login.

1 38. The method as claimed in claim 36 wherein said event type is a ping.

1 39. The method as claimed in claim 32 further comprising generating a
2 report of all new events which occur over a predetermined time period.

1 40. The method as claimed in claim 39 wherein an event is identified as a
2 new event by:

3 determining whether said event is included in a single data structure with
4 one or more previous events received in a time period preceding said
5 predetermined time period;
6 searching all data structures generated during said time period preceding
7 said predetermined time period if said event is not included in said single data
8 structure with one or more previous events; and
9 including said event in said report if said event is not identified in any
10 data structures generated during said time period preceding said predetermined
11 time period.